Change Date	Change Description	Booklets Changed	Comment
06/30/21	Revised the Operations Booklet and Changed Name to Architecture, Infrastructure, and Operations	Architecture, Infrastructure, and Operations (AIO)	▪ Changed booklet name to from Operations to Architecture, Infrastructure, and Operations to reflect an increased focus on principles-based, enterprise-wide, process-oriented approaches that consider the design of technology within the overall business structure (architecture), including implementation of IT infrastructure components (infrastructure), and delivery of services to provide security and value for internal and external customers (operations). ▪ The most significant changes to the booklet include the additions of new sections: architecture, infrastructure, and emerging technology, including cloud computing, to the narrative. ▪ Cybersecurity is incorporated throughout the booklet as a consideration for all technology employed by entity management, whether managed internally or contracted for from a third-party service provider. ▪ Within the narrative, we have developed a new section for governance and common risk management elements of architecture, infrastructure, and operations (AIO) as well as sections that contain specific risks applicable to architecture, infrastructure, and evolving technologies. ▪ In keeping with our approach for all booklet revisions and as seen in the BCM

Change Date	Change Description	Booklets Changed	Comment
			booklet, the booklet was drafted with a more principles-based approach to the narrative.
			▪ In the Common AIO Risk Management Topics section, we included risk management discussions that include risks that affect each of the entity's AIO functions.
			▪ In the Architecture section, we added discussions relating to strategic planning of the IT architecture design to integrate with the business functions of the enterprise, and provide for service delivery to customers.
			▪ In the Infrastructure section, we included sections on hardware, network and telecommunications, software, environmental controls, and physical access controls.
			▪ The Operations section was updated to address key operational principles in IT environments. We included discussions of operational controls, IT operational processes, service and support processes, and ongoing monitoring and evaluation processes.
			▪ The purpose of the Evolving Technologies section is to provide examiners with general information relating to newer technologies and topics that they may encounter during examinations.

Change Date	Change Description	Booklets Changed	Comment
			▪ We continued to make improvements in consistency and use of authoritative standards for the revision of booklets in the following ways: 1) Identified clearer references back to NIST and other authoritative sources; 2) Replaced "financial institutions" with the term "entities" as the principles in the narrative also apply to third-party service providers and significant service providers that we examine; 3) Aligned definitions and terminology with authoritative sources and standards organizations (e.g., NIST), where appropriate; 4) Included joint/interagency guidance applicable to AIO and accompanying respective agency announcements for consistency.
10/24/19	Revised the Business Continuity Planning Booklet and Changed Name to Business Continuity Management	Business Continuity Management (BCM)	▪ Changed name to Business Continuity Management to reflect an increased focus on ongoing, enterprise-wide business continuity and resilience. ▪ Replaced the term "financial institutions" with the term "entities." ▪ Clearer references back to NIST, FEMA, and other authoritative sources. ▪ Clarified the linkage between enterprise risk management (ERM) and BCM. ▪ Eliminated the redundant pandemic planning section. ▪ Discussed supply-chain risk with respect to single points of failure.

Change Date	Change Description	Booklets Changed	Comment
			▪ Clarified the distinction between exercises and tests. ▪ Elevated maintenance and improvement as an important component of the BCM lifecycle. ▪ Integrated relevant concepts from Appendix J into the body of the booklet. ▪ Aligned definitions and terminology with authoritative standards organizations (e.g., NIST and ISO), where appropriate.
09/09/16	Revised the Information Security Booklet	Information Security	The updates included the removal of redundant management material and a refocus on IT risk management and an update of information security processes. The revision reflects changes in the industry. It also streamlined and reordered information security concepts throughout the booklet. The updates are consistent with the FFIEC Cybersecurity Assessment Tool (CAT) and the NIST Cybersecurity Framework as appropriate. The booklet contains updated examination procedures to help examiners measure the adequacy of an institution's culture, governance, information security program, security operations, and assurance processes.
04/29/16	Added Appendix E to address Mobile Financial Services (MFS)	Retail Payment Systems	The update consists of the addition of a new appendix, *Appendix E: Mobile Financial Services.* Appendix E focuses on the risks associated with MFS and emphasizes an enterprise-wide risk management approach

Change Date	Change Description	Booklets Changed	Comment
			to effectively manage and mitigate those risks. The update included the following: • A workprogram specific to MFS. • An update to the glossary to incorporate terminology in the appendix. The other sections of the booklet remain unchanged.
11/10/15	Revised the Management Booklet	Management	Full revision of the Management Booklet; replaces the June 2004 version. Includes revised workprogram.
02/06/15	Added Appendix J to address Strengthening the Resilience of Outsourced Technology Services	Business Continuity Planning (BCP)	The appendix highlights and strengthens the BCP Booklet in four specific areas: Third-Party Management, Third-Party Capacity, Testing with Third-Party TSPs, and Cyber Resilience. Financial institutions should partner with their TSPs as needed to strengthen the resilience of outsourced technology as recommended through this guidance.
04/02/14	Added FFIEC Statement on DDoS Threat	N/A	Identifies risks and mitigation strategies
04/02/14	Added FFIEC Statement on Cyber Attacks – ATM's & Card Systems	N/A	Discusses the possible threat to ATM's and their related Card Systems.
10/07/13	Added FFIEC Statement on Windows XP End of Life	N/A	Discusses risks and need to take action.
03/22/13	Added user E-mail and/or RSS notification of changes	N/A	Notifies users of additions, changes, and deletion of content

Change Date	Change Description	Booklets Changed	Comment
10/31/12	Revised the Supervision of Technology Service Providers Handbook	Supervision of Technology Service Providers (TSP)	Replaces the March 2003 version
10/31/12	Added Federal Regulatory Agencies' Administrative Guidelines on the implementation of Interagency Programs for the Supervision of Technology Service Providers	N/A	Reference Material Section Guidance for FRS, FDIC, and OCC agencies to implement the interagency supervisory programs and includes the reporting templates examiners use throughout the supervisory cycle
07/10/12	Added the FFIEC Cloud Computing Statement	N/A – Reference Material Section	Maps risks to FFIEC IT Booklets
05/07/12	Revised multiple booklets to address the transition from SAS-70 to the SSAE-16 attestation review process and other third-party review processes.	Audit, BCP, E-Banking, Information Security, Operations, Outsourcing, and Retail Payments.	Generally, the term SAS-70 was changed to embrace a broader set of review processes.
04/27/12	Added the FFIEC Supplement to Authentication in an Internet Environment to Appendix C (resource).	Information Security	Issued June 29, 2011
04/09/12	Added Appendix D to address the risks associated with outsourcing IT Security. Outsourcing	Includes Examination Procedures and Request Letter criteria	
04/02/12	Modified Appendix A to address the risks associated with Cloud Computing.	Outsourcing	